

Daniel W. Roberts,  
President

## *Roberts & Ryan Investments Inc.*

Based in San Francisco, we provide “value added” information to our global asset managing clients.

Serving Investors since 1987

### About Roberts & Ryan

We thank our readers for their support of our research efforts. Via this newsletter to our clients, we publish the smallest voices from Silicon Valley, California. Our contribution is to refute or confirm what is being publicly asserted by the covered companies. Thanks again.

In order to facilitate our receipt of directed order flow, we show our list of agents as follows:

Global markets:  
Merrill Lynch  
Societe Generale

(Pan European only)  
Cheuvreux

(Asia only)  
HSBC

(Australia only)  
Deutsche Bank

## Europe

### eBay retools fees to lure casual sellers

eBay hopes to lure more sellers by essentially doing away with “listing” fees for people who occasionally auction items on its site. Instead, it will take a cut of the final selling price.

eBay has tinkered with its fee structure in recent years in hopes of improving the experience people have on its site and reinvigorating its growth. Changes like the ones being announced Tuesday are meant to encourage more people to list items for sale.

eBay told sellers Tuesday that starting March 30 they will be able to post up to 100 items for auction every 30 days without paying fees if list them. The items must have a starting bid of less than \$1, and when they sell eBay will take 9 percent of the final price or \$50, whichever is

less.

Currently, eBay lets occasional sellers—who make up the majority of the 28 million people who sell on its main site— auction up to five items for free every 30 days. It



charges them 8.75 percent of the final price or \$20, whichever is less.

For sellers that only auction the occasional vintage Pez dispenser or designer handbag, Tuesday’s change could mean they pay eBay more. But Lorrie Norrington, the president of eBay Marketplaces,

thinks the change will be easier overall for people who want to auction off items that are sitting around the house. “Our customers have consistently told us, ‘We love free and we love simple,’

and that’s what we think these changes are about,” she said.

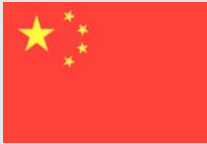
eBay made a similar change in fees in some European markets in 2008.

Once sellers exhaust the number of items they can list for free, they are subject to listing fees and commissions that vary, depending on the starting price of the item and the price at which it sells. Those listing fees are also changing for most auctions—to a range of 15 cents to \$2, depending on the item’s starting price. Right now, they generally range from 15 cents to \$4.

[www.robertsryan.net](http://www.robertsryan.net)

Roberts & Ryan Investments Inc., a Service Disabled Veterans Enterprise  
57 Post Street, Suite 614 San Francisco, CA 94104  
(415)956-2000, Toll Free (800)676-6717, Fax (415)296-8873  
Please Visit us @ [www.robertsryan.net](http://www.robertsryan.net)

# China



“A hacker attack reportedly from China infuriated Google, provoking a larger fight over China’s censorship of Internet content.”

## Attack on Google in China sheds light on Web security

The recent hacking attack that prompted Google’s threat to leave China is underscoring the heightened dangers of previously undisclosed computer security flaws— and renewing debate over buying and selling information about them in the black market. Because no fix was available, the linchpin in the attack was one of the worst kinds of security holes. Criminals treasurer these types of “zero day” security vulnerabilities because they are the closest to a sure thing and virtually guarantee the success of a shrewdly crafted attack.

The attackers waltzed into victims’ computers, like burglars with a key to the back door, by exploiting such a zero-day vulnerability in Microsoft’s Internet Explorer browser. Microsoft rushed out a fix after learning of the attack. How did the perpetrators learn about the flaw? Most likely, they merely had to tap a thriving underground market, where a hole “wide enough to drive a truck through” can command hundreds of thousands of dollars, said Ken Silva, chief technology officer of VeriSign. Such flaws can take months of fulltime hacking to find.

“Zero days are the safest for attackers to use, but they’re also the hardest to find,” Silva said. “If it’s not a zero day, it’s not valuable at all.”

The Internet Explorer flaw used in the attack on Google required tricking people into visiting a malicious Web site that installed harmful software on victims’ computers.

The attack, along with a discovery that computer hackers had tricked human-rights activists into exposing their Google e-mail accounts to outsiders, infuriated Google and provoked a larger fight over China’s censorship of the Internet content. Google has threatened to shut down its censored Chinese-language search engine and possibly close its offices in China.

Pedram Amini, manager of the Zero Day Initiative, at the security firm TippingPoint, estimated that the IE flaw could have fetched as much as \$40,000. He said even more valuable zero-day flaws are ones that can infect computers without any action on the user’s part. “Zero day” refers to security vulnerabilities caused by program-

ming errors that haven’t been “patched,” or fixed, by the products’ developers. Often those companies don’t know the weaknesses exist and have had zero days to work on closing the holes.

Microsoft knew about the flaw in this case since September but hadn’t planned to fix it until February, as companies sometimes prioritize fixing other problems and wait on the ones they haven’t seen used in attacks. Microsoft often fixes multiple vulnerabilities at once because testing patches individually is time-consuming and costly, said Chris Wysopal, co-founder of security company Veracode.

But criminals know how the patch cycle works, and Wysopal said the Google attackers may have realized their zero-day flaw was getting old—and thus stuck in December just before they thought Microsoft was going to fix it.

“They likely thought the bug would be fixed in January or February,” he said. “They were right.” Microsoft certainly could have fixed the bug earlier and prevented it from being used on Google, but security experts caution that an adversary that is well-funded or determined could have easily found another bug to use.

“Zero day aren’t difficult to find,” said Steven Santorelli, former Microsoft security research who works with Team Cymru, a nonprofit research group. “You don’t have to have a Ph.D. in computer science to find a zero-day exploit. It really is a factor of the amount of energy and effort you’re willing to put in.”

VeriSign’s iDefense Labs and 3Com’s TippingPoint division run programs that buy zero-day vulnerabilities from researchers in the so-called “white market.” They alert the affected companies without publicly disclosing the flaw and use the information to get a jump on rivals on building protections into their security products. There’s also another, highly secretive market for zero days: U.S. and other government agencies, which vie with criminals to offer the most money for the best vulnerabilities to improve their military and intelligence capabilities and shore up their defenses.

[www.robertsryan.net](http://www.robertsryan.net)

Roberts & Ryan Investments Inc., a Service Disabled Veterans Enterprise

This is a timely newsletter for our institutional clients. The information herein has been assembled with the utmost attention to detail, however as with all research, the accuracy cannot be guaranteed.

## South Korea

### Rambus wins \$900 million

In a huge victory for Los Altos-based Rambus, South Korean giant Samsung Electronics—one of three semiconductor companies Rambus has accused of trying to sabotage its business—agreed Tuesday to pay Rambus about \$900 million over the next five years to settle legal differences.

Rambus' CEO Harold Huges called the agreement "transformational" for his company of about 300 employees, which has been battling giant Samsung over other chipmakers for years over Rambus' chip technology and related issues. "This deal confirms both the power of our patents and the validity of our business model," he added. "It's impacts are profound from bottom to top."

In a joint statement with Rambus, Samsung, which did not admit wrongdoing, said it was "pleased to resolve their differences and move forward." Under the agreement, Samsung will invest \$200 million in Rambus stock and also pay the company \$200 million in cash, plus quarterly payment of about \$25 million over the next five years. The two companies also agreed to work together to develop new chips.

"It's a very big deal's for Rambus, said Capstone Investments analyst Jeff Schreiner,

adding that the two companies' agreement to collaborate on future chips could yield an even bigger revenue stream for Rambus. The settlement was announced as Rambus was about to go to trial in San Francisco against Samsung, Hynix Semiconductor of South Korea and Micron Technology of Idaho, all of whom had been accused by Rambus of plotting a damage Rambus' business. Rambus executives said they would be willing to discuss similar settlements with Hynix and Mircon.

However, in a prepared statement, Micro said, "We do not anticipate this settlement will have any impact on our ongoing litigation with Rambus" and that Micro believes Rambus' claims against it "are baseless."

Hynix officials could not be immediately reached for comment.

After its incorporation in 1900, Rambus developed a new technology for dynamic random access memory, or DRAM, chips, which provide high-speed storage and retrieval of data from personal computers another devices.

Claiming its design enabled the chips to keep up with the increasing speed of advanced microprocessors, Rambus persuaded a number of chipmakers to license its technology.

But Rambus claims Hynix, Samsung and Micro—which were pushing an alternative DRAM design they believed would yield them more profit—tired to make Rambus' version unattractive to computer makers by conspiring to limit the supply and boost the price of chips based on Rambus' architecture.

In recent years, U.S. prosecutors also accused some DRAM chipmakers of price-fixing, resulting in Hynix, Samsung and some other companies paying fines totaling several hundred million dollars. In court papers, Samsung, Micron and Hynix have denied Rambus' allegations and accused it of obliterating thousands of documents favorable to them.

Rambus, which denies that charge, also had been accused by U.S. and European regulators of trying to monopolize the DRAM market and charging unreasonable royalties by patenting its technology and then hiding those patents from a group that adopted Rambus' technology as an industry standard. But those probes were dropped last year, with Rambus promising European authorities to scale back its royalty demands.



"Under the agreement, Samsung will invest \$200 million in Rambus stock and also pay the company \$200 million in cash, plus quarterly payment of about \$25 million over the next five years."



[www.robertsryan.net](http://www.robertsryan.net)

Roberts & Ryan Investments Inc., a Service Disabled Veterans Enterprise

This is a timely newsletter for our institutional clients. The information herein has been assembled with the utmost attention to detail, however as with all research, the accuracy cannot be guaranteed.

# China

## Journalists say Gmail accounts were hacked



“We remind all members that journalists in China have been particularly targets of hacker attacks in the last two years. Please be very careful what you click on, and run virus checks regularly. ”

International journalists in China said that their Google e-mail accounts have been hacked in attacks similar to the ones against human rights activists that the search giant cited as a reason for considering pulling out of the country. In announcing a possible exit from China last week, Google did not specify how the accounts with its Gmail service were hacked into or by whom.

The Foreign Correspondents' Club of China sent an e-mail Monday to its members warning that reporters in at least two news bureaus in Beijing said their Gmail accounts had been broken into, with their e-mails surreptitiously forwarded to unfamiliar accounts. Although the warning did not name the organizations, one of the accounts belonged to an Associated Press journalist.

John Daniszewski, senior managing editor for international news at the news cooperative in New York, Associated Press will be investigating to determine if any vital information was compromised. The foreign correspondents' club asked its members to be vigilant in protecting their e-mail accounts and computers from attack.

“We remind all members that journalists in China have been particular targets of hacker attacks in the last two years,” the

club's message read. “Please be very careful what you click on, and run virus checks regularly.” Google's announcement last week that it might quit the huge Chinese market shocked the international business community and cheered many free-speech advocates. Google said a sophisticated attack in December from China targeted the Mountain View company's infrastructure and at least 20 other major companies from the Internet, Financial services, technology, media and chemical industries.

Google said only two e-mail accounts were infiltrated in the attacks, with basic information such as subject lines and the dates that the individual accounts were created accessed. In its investigation, Google said it found that dozens of accounts of human rights advocates in China, the U.S. and Europe were routinely accessed by third parties, not due to a security breach at Google, but through viruses and spy software secretly placed on the users' computers.

The tactics used against the journalists are similar to those described by one human rights activist. After Google's announcement, Beijing law professor and human rights lawyer Teng Biao wrote on his blog that someone broke into his Gmail account and forwarded

e-mails to another account. The attack made use of a service that Gmail and other Web-based e-mail services offer, allowing users to set e-mail addresses to which their mail can be forwarded automatically.

Another activist said she was notified by David Drummond, Google's top lawyer, on Jan 7 about an intrusion into her account. Tenzin Selfon, a Tibetan rights activist and sophomore at Stanford University, said she allowed her laptop to be inspected by Google's experts, who found no viruses on the machine.

China-based international correspondents have been their e-mail accounts hit by periodic waves of cyberattacks and snooping from undetermined sources over the past two years. The Associated Press, Agence France-Presse, Dow Jones, Reuters and other news organizations were targeted in September in an attack in which viruses were implanted in ordinary looking e-mails.

The e-mails, which appeared to be from an editor of an English-language paper in Singapore, bore an attachment that once opened would install malware—malicious software—on computers, said a report late last year by computer security experts at McAfee.



[www.robertsryan.net](http://www.robertsryan.net)

Roberts & Ryan Investments Inc., a Service Disabled Veterans Enterprise

This is a timely newsletter for our institutional clients. The information herein has been assembled with the utmost attention to detail, however as with all research, the accuracy cannot be guaranteed.